(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 49 970 A 1**

(51) Int. Cl.[7]:
G 07 C 11/00
E 05 B 47/00
H 04 B 5/00
G 08 C 17/02

(21) Aktenzeichen: 199 49 970.5
(22) Anmeldetag: 16. 10. 1999
(43) Offenlegungstag: 19. 4. 2001

(71) Anmelder:
Volkswagen AG, 38440 Wolfsburg, DE; Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Nemetschek, Dominique, 38110 Braunschweig, DE; Titze, Andreas, 38118 Braunschweig, DE; Meier, Michael, 31141 Hildesheim, DE; Schmitz, Stephan, 50672 Köln, DE

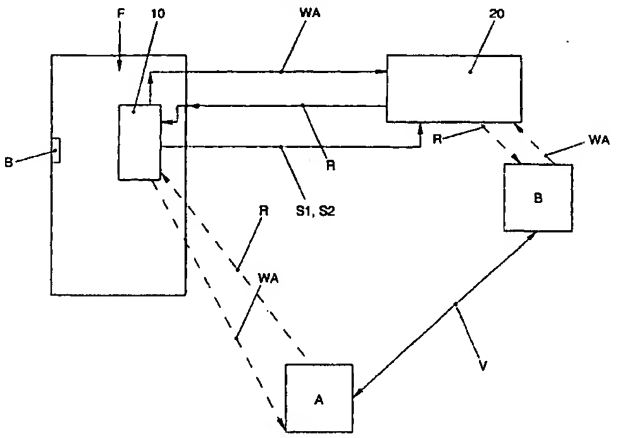
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	198 36 957 C1
DE	44 09 167 C1
DE	198 18 158 A1
DE	198 02 526 A1
DE	196 32 025 A1
DE	44 40 855 A1
DE	42 26 053 A1
DE	40 03 280 A1
US	58 83 443
EP	06 59 963 A1
WO	00 05 696 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort, insbesondere einem Kraftfahrzeug

(57) Die Erfindung betrifft ein Verfahren zur Zugangskontrolle zu einem gesicherten Ort, insbesondere zu einem Kraftfahrzeug (F), bei dem zwischen einem elektronischen Schlüssel (20) und einer Basisstation (10) in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen (10, 20) drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation (10) an den elektronischen Schlüssel (20) ein Aufrufsignal (WA) sendet und dieser auf das Aufrufsignal (WA) mit einem Antwortsiganal (R) antwortet, und wobei im aktiven Kommunikationsmodus eine Sicherungsprozedur gegen eine Funkstreckenverlängerung (V) durchgeführt wird.
Erfindungsgemäß ist vorgesehen, daß die Basisstation (10) das von ihr empfangene Antwortsignal (R) des elektronischen Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im aktiven Kommunikationsmodus empfangen wurde, an den elektronischen Schlüssel (20) einen ersten Selektionsbefehl (S1) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) an den elektronischen Schlüssel (10) einen zweiten Selektionsbefehl ...



DE 199 49 970 A 1

DE 199 49 970 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort, insbesondere zu einem Kraftfahrzeug, bei dem zwischen einem elektronischen Schlüssel und einer Basisstation in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation an den elektronischen Schlüssel ein Aufrufsignal sendet und dieser auf das Aufrufsignal mit einem Antwortsignal antwortet, und wobei im aktiven Kommunikationsmodus eine Sicherungsprozedur gegen eine Funkstreckenverlängerung durchgeführt wird, sowie eine Vorrichtung zur Durchführung dieses Verfahrens.

Ein Verfahren und eine Vorrichtung der eingangs genannten Art sind in der älteren internationalen Patentanmeldung PCT/DE99/02178 beschrieben. Hierbei ist vorgesehen, daß die zwischen dem elektronischen Schlüssel und der Basisstation ablaufende Sicherungsprozedur derart erfolgt, daß im aktiven Betriebsmodus die Kommunikation zwischen dem elektronischem Schlüssel und der Basisstation über UHF-Frequenzen erfolgt, wobei die Reichweite der Übertragung zwischen dem elektronischen Schlüssel und der Basisstation begrenzt ist, um zu gewährleisten, daß die Kommunikationsverbindung unterbrochen wird, wenn sich die im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des gesicherten Ortes, z. B. des Kraftfahrzeugs, entfernt.

Um nun zu verhindern, daß ein derartiges passives Zugangskontrollsystem nicht dadurch außer Kraft gesetzt wird, daß ein unbefugter Angreifer das von der Basisstation ausgesandte Aufrufsignal an den elektronischen Schlüssel abfängt, das abgefangene Signal über eine Funkstreckenveränderung an einen weiteren Angreifer, der sich in der Nähe des elektronischen Schlüssels befindet, weitersendet und der weitere Angreifer dann das Antwortsignal des elektronischen Schlüssels auf das Aufrufsignal der Basisstation über die Funkstreckenverlängerung wieder zurück zum ersten Angreifer und über diesen zurück zur Basisstation sendet, ist bei dem bekannten Verfahren vorgesehen, daß der elektronische Schlüssel der Basisstation ein Signal übermittelt, das von der Basisstation in spektrale Daten umgesetzt wird. Die Basisstation gewährt dann nur Zugang zu dem gesicherten Ort, wenn bei der Übertragung der Authentifizierungsdaten diese spektralen Daten mit einer in der Basisstation gespeicherten spektralen Signatur des elektronischen Schlüssels übereinstimmen. Hierbei ist vorgesehen, daß das von dem elektronischen Schlüssel ausgesandte Signal mindestens zwei Töne mit unterschiedlichen Frequenzen f_1 bzw. f_2 umfaßt, und daß die spektralen Daten Töne dritter Ordnung des übermittelten Signals darstellen, die von der Basisstation auf den Frequenzen $2f_1$-f_2 und $2f_2$-f_1 gemessen wird. Liegt die empfangene Signalstärke dieser Nebenlinien des vom elektronischen Schlüssel ausgesandten Signals über einem vordefinierten Wert, so interpretiert dies die Basisstation als sicheres Anzeichen dafür, daß eine Funkstreckenverlängerung durchgeführt wurde, und verweigert den Zugang zum gesicherten Ort.

Um beim Ausfall des aktiven Kommunikationsmodus im Rahmen eines sogenannten Back-up-Modus, also eines passiven Kommunikationsmodus, dem Benutzer der elektronischen Zugangskontrolle noch die Möglichkeit zu geben, den gesicherten Ort betreten zu können, ist vorgesehen, daß in diesem passiven Kommunikationsmodus eine Datenübertragung zwischen dem elektronischen Schlüssel und der Basisstation durch eine passive Modulation des von der Basisstation ausgesandten Erregerfeldes erfolgt: Der elektronische Schlüssel verstimmt entsprechend den zu sendenden Daten seinen Ressonanzkreis, was von der Basisstation als zusätzliche Belastung ihres Schwingkreises gemessen werden kann. Diese auf LF-Frequenzen erfolgende passive Kommunikation ist auf wenige Zentimeter beschränkt, was bedeutet, daß ein potentieller Angreifer seine entsprechende Antenne sehr nahe an die Sendeantenne der Basisstation plazieren muß, um in diesem Back-up-Modus zu arbeiten, wenn er versucht, die vom Schlüssel ausgesandten Datensignale auf einer LF-Frequenz im Back-up-Modus an die Basisstation zu senden. Das bekannte Verfahren sowie die nach diesem Verfahren arbeitenden bekannten Vorrichtungen besitzen den Nachteil, daß sie keinen wirksamen Schutz gegen einen auf diese vorgenannte Art und Weise erfolgenden Angriff bieten.

Es ist daher Aufgabe der Erfindung, ein Verfahren und eine Vorrichtung der eingangs genannten Art derart weiterzubilden, daß ein wirksamer Schutz gegen eine Funkstreckenverlängerung im passiven Kommunikationsmodus gegeben ist.

Diese Aufgabe wird durch das erfindungsgemäße Verfahren dadurch gelöst, daß die Basisstation das von ihr empfangene Antwortsignal des elektronischen Schlüssels daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal empfangen wurde, und daß die Basisstation für den Fall, daß das Antwortsignal des elektronischen Schlüssels im aktiven Kommunikationsmodus empfangen wurde, an den elektronischen Schlüssel einen ersten Selektionsbefehl sendet, welcher bewirkt, daß der elektronische Schlüssel die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal des elektronischen Schlüssels im passiven Kommunikationsmodus empfangen wurde, die Basisstation an den elektronischen Schlüssel einen zweiten Selektionsbefehl sendet, welcher bewirkt, daß der elektronische Schlüssel die nachfolgende Kommunikation im passiven Kommunikationsmodus ausführt.

Durch das erfindungsgemäße Verfahren wird in vorteilhafter Art und Weise erreicht, daß auch im passiven Kommunikationsmodus zwischen dem elektronischen Schlüssel und der Basisstation ein entsprechender Angriff einer nicht authorisierten Person abgewehrt werden kann, indem die Basisstation aktiv auf die Kommunikationsart, in der sie das Antwortsignal des elektronischen Schlüssels empfängt, reagiert. Wenn das Antwortsignal im aktiven Kommunikationsmodus erfolgt, wird das weitere Authentifizierungsverfahren im aktiven Kommunikationsmodus durchgeführt und eine Funkstreckenverlängerung kann durch die bekannte Sicherungsprozedur ausgeschlossen werden. Wenn aber die Basisstation das Antwortsignal des elektronischen Schlüssels im passiven Kommunikationsmodus empfängt, verhindert sie bis zum Abschluß der Zugangsprozedur in vorteilhafter Art und Weise eine Kommunikation zwischen Basisstation und Schlüssel über den ersten, aktiven Kommunikationsmodus. Es ist somit nicht möglich, daß ein Angreifer über eine Frequenz des aktiven Kommunikationsmodus eine Funkstreckenverlängerung durchführt.

Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Weitere Einzelheiten und Vorteile der Erfindung sind dem Ausführungsbeispiel zu entnehmen, das im folgenden anhand der einzigen Figur beschrieben wird. Es zeigt:

Fig. 1 eine Prinzipskizze eines Ausführungsbeispiels des des Verfahrens.

In **Fig. 1** ist nun die typische Konstellation dargestellt, die Ausgangspunkt des nachstehend beschriebenen Verfahrens zur Zugangskontrolle zu einem gesicherten Ort, hier zu einem Kraftfahrzeug F, ist. Im Kraftfahrzeug F ist eine Basis-

station **10** angeordnet, welche drahtlos mit einem elektronischen Schlüssel **20** Authentifizierungsdaten austauscht, um zu gewährleisten, daß nur der Besitzer des elektronischen Schlüssels **20** Zugang zu dem gesicherten Ort erhalten kann. Hierzu ist vorgesehen, daß die Basisstation **10** in einem aktiven, ersten Kommunikationsmodus ein Aufrufsignal WA für den elektronischen Schlüssel **20** aussendet, wenn ein Betätigungsorgan B, z. B. ein Türgriff, am Kraftfahrzeug F betätigt wird. Der elektronische Schlüssel **20** antwortet daraufhin im aktiven Kommunikationsmodus mit einem entsprechenden Antwortsignal R, womit eine in dem aktiven Kommunikationsmodus ablaufende Kommunikationsverbindung zwischen dem elektronischen Schlüssel **20** und der Basisstation **10** hergestellt ist. Die zwischen dem elektronischen Schlüssel **20** und der Basisstation **10** übermittelten Daten werden durch ein an und für sich bekanntes und daher nicht mehr näher beschriebenes Kommunikationsprotokoll bestimmt, welches der elektronische Schlüssel **20** und die Basisstation **10** befolgen und die Übermittlung von Authentifizierungsdaten vom elektronischen Schlüssel **20** an die Basisstation **10** beinhaltet. Der Zugang zu dem gesicherten Kraftfahrzeug F wird von der Basissation **10** nur dann zugelassen, wenn die vom elektronischen Schlüssel **20** übermittelten Authentifizierungsdaten mit den von der Basisstation **10** gespeicherten Authentifizierungen übereinstimmen. Hierbei ist vorgesehen, daß die vom elektronischen Schlüssel **20** und/oder von der Basisstation **10** ausgesandten Signale nur eine begrenzte Reichweite aufweisen, um zu verhindern, daß von der Basisstation **10** Zugang zu dem gesicherten Kraftfahrzeug F auch dann gewährt wird, wenn sich der elektronische Schlüssel **20** nicht innerhalb einer definierten Umgebung – typischerweise einige wenige Meter – des Kraftfahrzeugs F befindet.

Um nun zu verhindern, daß sich Angreifer zu dem gesicherten Kraftfahrzeug F dadurch Zugang verschaffen, daß ein erster Angreifer A das von der Basisstation **10** im ersten, aktiven Kommunikationsmodus ausgesandte Aufrufsignal WA mittels einer Funkstreckenverlängerung V zu einem zweiten Angreifer B leitet, dieser daraufhin das Aufrufsignal WA der Basisstation **10** an den sich außerhalb der Reichweite der Basisstation **10** befrndliche elektronische Schlüssel **20** leitet, das Antwortsignal R des elektronischen Schlüssels **20** auffängt, über die Funkstreckenverlängerung V dem ersten Angreifer A weiterleitet und dieser dann das Antwortsignal R des elektronischen Schlüssels **20** an die Basisstation **10** weiterleitet, ist vorgesehen, daß die zwischen dem elektronischen Schlüssel **20** und der Basisstation **10** im ersten, aktiven Kommunikationsmodus stattfindenden Kommunikation auch eine Sicherheitsprozedur aufweist, welche es gestattet, eine derartige Funkstreckenverlängerung V der entsprechenden Signale WA, R zu erkennen und gegebenenfalls daraufhin die Kommunikation abzubrechen. Eine derartige Sicherheitsprozedur ist z. B. in der älteren internationalen Patentanmeldung PCT/DE99/02178 beschrieben, auf die zur Vermeidung von Wiederholungen bezug genommen wird und deren Offenbarung durch diese Bezugnahme explizit zum Gegenstand der hier vorliegenden technischen Lehre gemacht wird. Sie wird dort dadurch realisiert, daß der elektronische Schlüssel **20** im Rahmen seines als Reaktion auf das Aufrufsignal WA der Basisstation **10** generierten Antwortsignals R ein Kennungssignal übermittelt, das die Basisstation **10** in spektrale Daten umsetzt und nur dann die Kommunikation mit dem elektronischen Schlüssel **20** fortsetzt, wenn die von ihr empfangenen spektralen Daten mit der spektralen Signatur des elektronischen Schlüssels **20**, die in der Basisstation **10** gespeichert ist, übereinstimmt. Insbesondere ist hierbei vorgesehen, daß der elektronische Schlüssel **20** zwei Töne mit der Frequenz f_1 bzw. f_2 aussendet, die nachher von der Basisstation **10** gemessen werden. Es werden aber nicht nur die beiden Töne f_1 und f_2, sondern auch Mischungen der beiden Grundtöne höherer Ordnung empfangen, welche in von den Grundtönen frequenzmäßig separierten Frequenzkanälen empfangen werden. Wenn nun die empfangene Signalstärke insbesondere der Nebenlinien dritter Ordnung über einem vordefinierten Wert liegt, ist das ein sicheres Indiz dafür, daß das empfangene Signal des elektronischen Schlüssels **20** über eine Funkstreckenverlängerung V geleitet wurde. In diesem Fall bricht dann die Basisstation **10** die Kommunikation mit dem elektronischen Schlüssel **20** ab und sperrt den Zugang zu dem gesicherten Kraftfahrzeug F.

Da aber üblicherweise vorgesehen ist, daß der elektronische Schlüssel **20** mit der Basisstation **10** nicht nur über im vorstehend beschriebenen aktiven Kommunikationsmodus, sondern auch im sogenannten Back-up-Modus in einem zweiten, passiven Kommunikationsmodus miteinander zu kommunizieren in der Lage sein sollen, ist es erforderlich, auch in diesem passiven Kommunikationsmodus, in dem die Sicherungsprozedur des aktiven Kommunikationsmodus nicht funktioniert, eine weitere Sicherungsprozedur für eben diesen passiven Kommunikationsmodus vorzusehen.

Dies wird in vorteilhafter Art und Weise dadurch erreicht, daß die Basisstation **10** nicht nur den Informationsgehalt der ihr zugeführten Signale, insbesondere des Antwortsignals R des Schlüssels **20** auswertet, sondern auch untersucht, ob die ihr zugeführten Signale des elektronischen Schlüssels **20** im ersten, aktiven Kommunikationsmodus oder im zweiten, passiven Kommunikationsmodus empfangen werden. Empfängt die Basisstation **10** das als Reaktion auf einen von ihr ausgesandten Aufrufbefehl WA vom elektronischen Schlüssel **20** generierte Antwortsignal R im ersten, aktiven Kommunikationsmodus, so sendet sie als Reaktion auf das im aktiven Kommunikationsmodus erhaltene Antwortsignal R des elektronischen Schlüssels **20** an diesen ein erstes Selektionssignal S1, welches – neben den üblichen Funktionen eines Selektionssignals – bewirkt, daß zumindest die sicherheitsrelevante und vorzugsweise die gesamte weitere Kommunikation zwischen dem elektronischen Schlüssel **20** und der Basisstation **10** ausschließlich im ersten, aktiven Kommunikationsmodus durchgeführt wird und die Durchführung des verbleibenden Authentifizierungsprozesses im passiven Kommunikationsmodus unterbunden wird. Dies hat den Vorteil, daß eine Funkstreckenverlängerung V durch die Sicherungsprozedur des aktiven Kommunikationsmodus detektierbar ist und gegebenenfalls entsprechende Maßnahmen gegen einen Angriff einer nicht-authorisierten Person vorgenommen werden können.

Empfängt jedoch die Basisstation **10** des Kraftfahrzeugs F das Antwortsignal R des elektronischen Schlüssels **20** im zweiten, passiven Kommunikationsmodus, so sendet sie als Reaktion darauf an den elektronischen Schlüssel **20** ein zweites Selektionssignal S2, welches in entsprechender Art und Weise bewirkt, daß die Kommunikation des weiteren Authentifizierungsvorgangs im zweiten, passiven Kommunikationsmodus durchgeführt wird, und eine Durchführung des verbleibenden Authentifizierungsvorgangs im ersten Kommunikationsmodus unterbunden wird. Es ist somit einem eine im aktiven Kommunikationsmodus arbeitende Funkstreckenverlängerung V verwendenden Angreifer nicht mehr möglich, diese erfolgreich einzusetzen.

Patentansprüche

1. Verfahren zur Zugangskontrolle zu einem gesicherten Ort, insbesondere zu einem Kraftfahrzeug (F), bei dem zwischen einem elektronischen Schlüssel (**20**) und

einer Basisstation (10) in einem aktiven oder einem passiven Kommunikationsmodus diese Einrichtungen (10, 20) drahtlos Authentifizierungsdaten austauschen, wobei zu Beginn dieses Authentifizierungsprozesses die Basisstation (10) an den elektronischen Schlüssel (20) ein Aufrufsignal (WA) sendet und dieser auf das Aufrufsignal (WA) mit einem Antwortsignal (R) antwortet, und wobei im aktiven Kommunikationsmodus eine Sicherungsprozedur gegen eine Funkstreckenverlängerung (V) durchgeführt wird, **dadurch gekennzeichnet,** daß die Basisstation (10) das von ihr empfangene Antwortsignal (R) des elektronischen Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im aktiven Kommunikationsmodus empfangen wurde, an den elektronischen Schlüssel (20) einen ersten Selektionsbefehl (S1) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die darauffolgende Kommunikation im aktiven Kommunikationsmodus ausführt, und daß für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) an den elektronischen Schlüssel (10) einen zweiten Selektionsbefehl (S2) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die nachfolgende Kommunikation im passiven Kommunikationsmodus ausführt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Sicherungsprozedur des aktiven Kommunikationsmodus dadurch ausgeführt wird, daß der elektronische Schlüssel (20) im Rahmen seines als Reaktion auf das Aufrufsignal (WA) der Basisstation (10) generierten Antwortsignals (R) eine Kennung an die Basisstation (10) übermittelt, welche die Basisstation (10) in spektrale Daten umsetzt und nur dann die Kommunikation mit dem elektronischen Schlüssel (20) fortsetzt, wenn die von ihr empfangenen spektralen Daten mit einer spektralen Signatur des elektronischen Schlüssels (20), die in der Basisstation (10) gespeichert ist, übereinstimmt.

3. Vorrichtung zur Zugangskontrolle zu einem gesicherten Ort (F), die eine Basisstation (10) und einen elektronischen Schlüssel (20) aufweist, wobei zwischen der Basisstation (10) und dem elektronischen Schlüssel (20) in einem aktiven oder passiven Kommunikationsmodus Authentifizierungsdaten ausgetauscht werden, wobei im aktiven Kommunikationsmodus die Basisstation (10) einer Sicherungsprozedur gegen eine Funkstreckenverlängerung (V) durchführt, dadurch gekennzeichnet, daß die Basisstation (10) ein von ihr empfangenes Antwortsignal (R) des elektronischen. Schlüssels (20) daraufhin untersucht, in welchem Kommunikationsmodus dieses Antwortsignal (R) empfangen wurde, und daß die Basisstation (10) für den Fall, daß das. Antwortsignal (R) des elektronischen Schlüssels (20) empfangen wird, einen ersten Selektionsbefehl (S1) erzeugt und an den elektronischen Schlüssel (20) sendet, wobei der erste Selektionsbefehl (S1) bewirkt, daß der elektronische Schlüssel (20) die darauffolgende Kommunikation mit der Basisstation (10) im aktiven Kommunikationsmodus ausführt, und daß die Basisstation (10) für den Fall, daß das Antwortsignal (R) des elektronischen Schlüssels (20) im passiven Kommunikationsmodus empfangen wurde, die Basisstation (10) einen zweiten Selektionsbefehl (S2) erzeugt und an den elektronischen Schlüssel (20) sendet, welcher bewirkt, daß der elektronische Schlüssel (20) die nachfolgende Kommunikation mit der Basisstation (10) im passiven Kommunikationsmodus ausführt.

4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß nach dem Empfang eines Selektionsbefehls (S1, S2) durch den elektronischen Schlüssel (20) dieser wenigstens die sicherheitsrelevanten Daten des Authentifizierungsprozesses in dem die empfangene Selektionsbefehle (S1, S2) entsprechenden Kommunikationsmodus durchführt.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß nach dem Empfang eines Selektionsbefehls (S1, S2) durch den elektronischen Schlüssel (20) dieser wenigstens den gesamten darauffolgenden Authentifizierungsprozess in dem die empfangene Selektionsbefehle (S1, S2) entsprechenden Kommunikationsmodus durchführt.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 199 49 970 A1
Int. Cl.[7]: G 07 C 11/00
Offenlegungstag: 19. April 2001

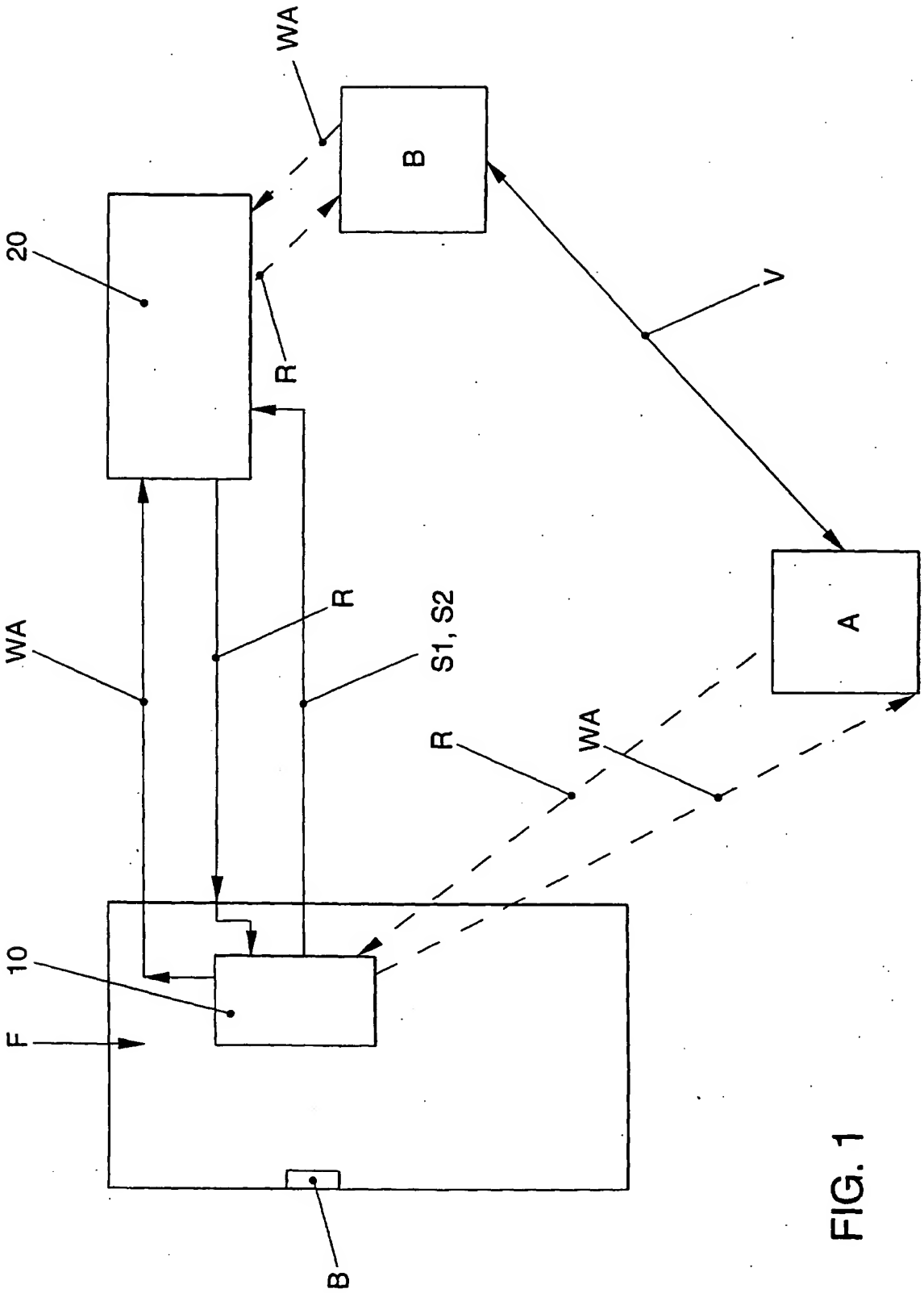


FIG. 1